

# 暗号プロトコルに関する 評価実証実験結果

株式会社 KDDI 研究所  
情報セキュリティグループ  
太田 陽基

**KDDI 研独自ツールによる評価  
(KDDI 研究所)**

## ➤ 基本情報

- 開発元: 株式会社 KDDI 研究所 (日本)
- ツールタイプ: モデルチェックツール
- 動作環境: Windows
- 参考文献: Haruki Ota, Shinsaku Kiyomoto, and Yutaka Miyake, "Fast and Automatic Verification of Authentication and Key Exchange Protocols"

## ➤ ツールの特徴

- GUI により、**直感的に**プロトコル情報を入力可能。
- 攻撃モデルを詳細に設定することなく、所望のセキュリティプロパティを**選択するだけで**、対象となる安全性を検証可能。
- セキュリティパラメータを設定可能で、データ長や鍵長がセキュリティパラメータに対して**十分な長さを有するか**を検証可能。
- 具体的な暗号アルゴリズムを設定可能で、対象となる暗号アルゴリズムが**危殆化していないか**を検証可能。
- 評価基準として PAL4 を前提にしているにも関わらず、安全性を**高速に**検証可能 (検証プロセスが止まらなくなることはなく、検証結果を必ず出力)。

## ➤ 言語仕様

- ツール自体は Java アプリケーションであるが、GUI による入出力が可能。 3

## ➤ ユーザーインターフェース

### ➤ 入力

- **GUI** により、基本情報、エンティティ、データ、関数、フローなどを入力。

### ➤ 出力

- 評価結果のみを示した**テキスト出力**及びプロトコルの入力情報、評価結果、詳細ログを示した **GUI 出力(レポートファイル出力)**がそれぞれ可能。
- 入力情報はシーケンス図と表により**わかりやすく**表示。
- 評価結果はプロトコル全体と**セキュリティプロパティごと**に OK/NG により出力。検証時間、長さと危殆化のチェック結果も出力。
- セキュリティプロパティが NG になった理由は詳細ログを読み解く必要あり。

## ➤ 評価可能性と記述の自由度

- プロトコル構成、データ・関数の種別、セキュリティプロパティなどが**固定されている**ため、入力可能なプロトコルに対しては**モデル記述が容易**。
- **定義されていない入力情報**を要するプロトコルの評価不可。評価可能なセキュリティプロパティは以下のとおり。
  - 認証: なりすまし攻撃安全と鍵漏洩なりすまし攻撃安全
  - 鍵交換: 受動的攻撃安全、能動的攻撃安全、既知鍵攻撃安全、未知鍵共有攻撃安全、weak forward secrecy、strong forward secrecy、鍵プライバシー
  - パスワードベース: オフライン辞書攻撃安全と検出不可能なオンライン辞書攻撃安全

The screenshot displays a software interface for a security tool. On the left is a tree view of a project named 'sample', containing folders for 'Entity', 'Data', and 'Flow'. The 'Data' folder is expanded, showing various cryptographic parameters like 'Identifier', 'Random Number', 'Pre-shared Key', etc. The main window is divided into three sections:

- シーケンス図 (Sequence Diagram):** Shows a protocol flow between two entities, C1 (K1) and C2 (K1).
  - Flow [1]: C1 sends R1 to C2.
  - Flow [2]: C2 sends R2, M1, R3 to C1.
  - Flow [3]: C1 sends M2 to C2.
- プロトコル入力情報 (Protocol Input Information):** A table showing the state of each entity at different points in the protocol.
 

Entity	Timing	Having data
C1	Initial	K1
C1	After flow[1]	K1, R1
C1	After flow[2]	K1, R1, R3
C1	After flow[3]	K1, R1, R2, R3
C2	After flow[1]	K1, M3, R1, R2
C2	After flow[2]	K1, M1, M3, R1, R2, R3
C2	After flow[3]	K1, M1, M2, M3, R1, R2, R3
- 検証結果 (テキストベース) (Verification Results):** A list of test results for various cryptographic checks.
  - fast verification process time: 12.61msec.
  - verification for authentication protocol: NG
  - verification for key exchange protocol: NG
  - check compromised: OK
  - check length: OK
  - MC-SIA: OK
  - MC-RKCI with C1: NG
  - MC-RKCI with C2: NG
  - SS-SPA: OK
  - SS-SAA: OK
  - SS-KKS: OK
  - SS-RUKS: OK
  - SS-WFS: NG
  - SS-SFS: NG
  - RDDA: N/A
  - RUDDA: N/A

## 基本情報設定

The screenshot shows the 'Document Settings' dialog box with the following sections and controls:

- Protocol Settings:** Protocol Name: sample
- Entity Number:** Radio buttons for 2, 3, 4, and Group. **Flow Data:**  Know Flow Data
- Group Controller:** Radio buttons for N/A, Static, and Dynamic
- Clients:** C1, C2, C3, ..., Cn-2, Cn-1, Cn
- Security Parameter:** 128
- Purpose:**  Authentication,  Key Exchange
- Security Properties:**
  - MC:**  MC-SIA,  MC-RKCI
  - SS:**  SS-SPA,  SS-SAA,  SS-KKS,  SS-RUKS,  SS-WFS,  SS-SFS,  SS-WBS,  SS-KP
- Common:**  RODA,  RUODA
- Comment:** Text area with scrollbars
- Buttons:** Apply, Cancel

セキュリティパラメータ

プロトコル種別

セキュリティプロパティ

## 関数設定

The screenshot shows the 'Function Parameters' dialog box with the following sections and controls:

- Function:** M(R1, R2|K... | MAC | HMAC-SHA-256 oid.1... | Name: M
- Number:** 1 | **Length:** 256 | **Key:** K1 | **鍵**
- Arguments:**
  - Data & Functions:** K1, M1, M2, M3, R3
  - Arguments:** R1, R2
  - 引数**
- Comment:** Text area with scrollbars
- Current Settings:** M1 (R1, R2|K1)[256]
- Buttons:** Apply, Close

関数種別

暗号アルゴリズム

鍵

引数

## レポートファイル

### sample プロトコル 評価レポート

#### プロトコル設定



シーケンス図

#### 名称

sample

#### セキュリティパラメータ

128

#### 別注

- 検証プロトコル: 用途あり
- 観交換プロトコル: 用途あり

## プロトコル入力情報

#### エンティティ

エンティティ	識別子	長さ	セッション	当番から持っているデータ
C1	M2(R3/K1)		M3(R2/K1)	K1
C2	M1(R1,R2/K1)		M3(R2/K1)	K1

#### データ

データ種別	名前	長さ	作成者
観	R1	128	C1
	R2	128	C2
	R3	128	C2
事前共有値	K1	128	C1

#### 観

名前	名前 (引数   値)	長さ	観別
M1	M1(R1,R2/K1)	256	メッセージ観コード(MAC)
M2	M2(R3/K1)	256	メッセージ観コード(MAC)
M3	M3(R2/K1)	256	メッセージ観コード(MAC)

#### フロー

名前	同期フロー	送信者	受信者	データ
フロー[1]	フロー-1	C1	C2	R1
フロー[2]	フロー-2	C2	C1	R2,M1(R1,R2/K1),R3
フロー[3]	フロー-3	C1	C2	M2(R3/K1)

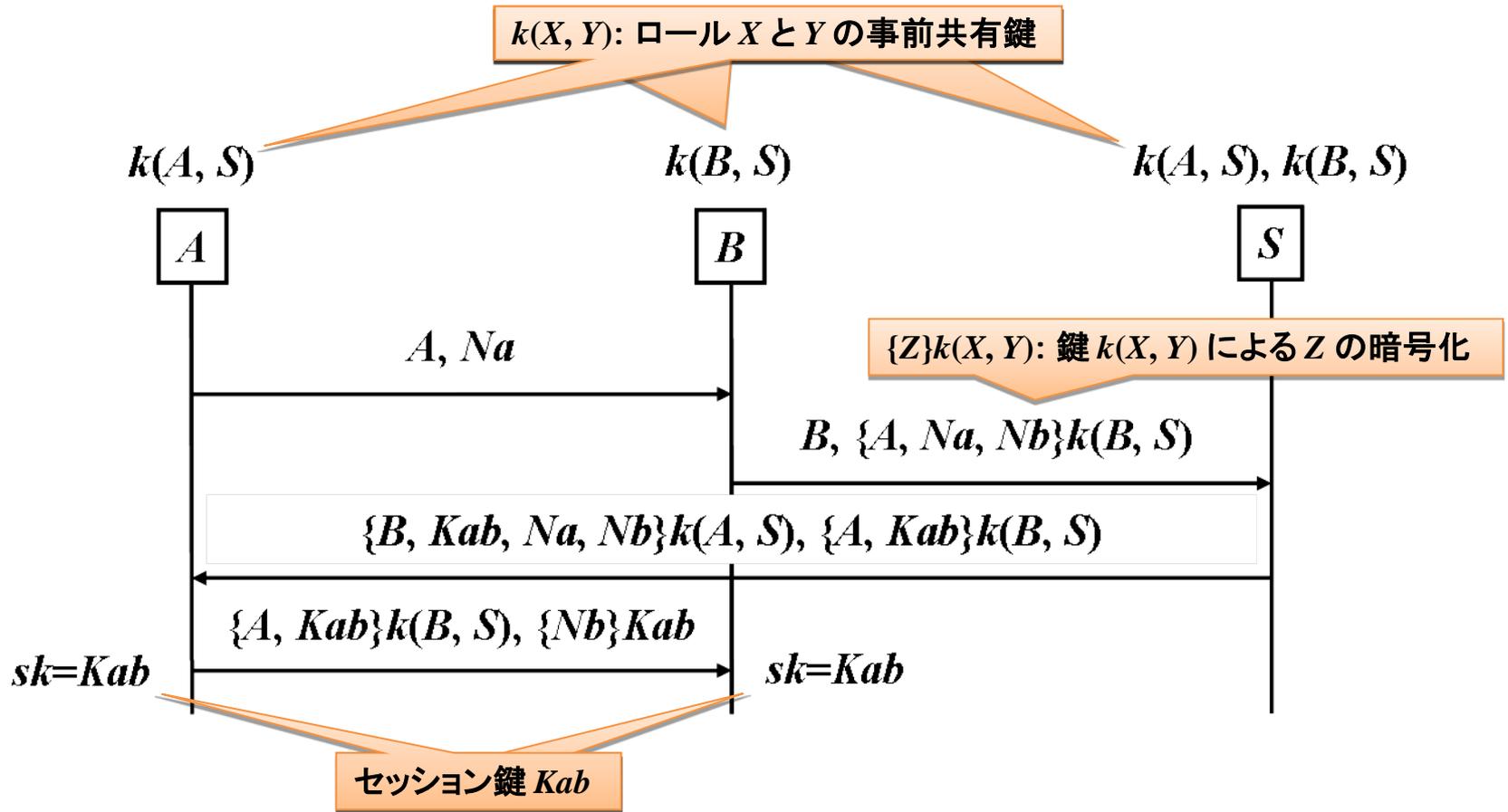
#### 評価結果

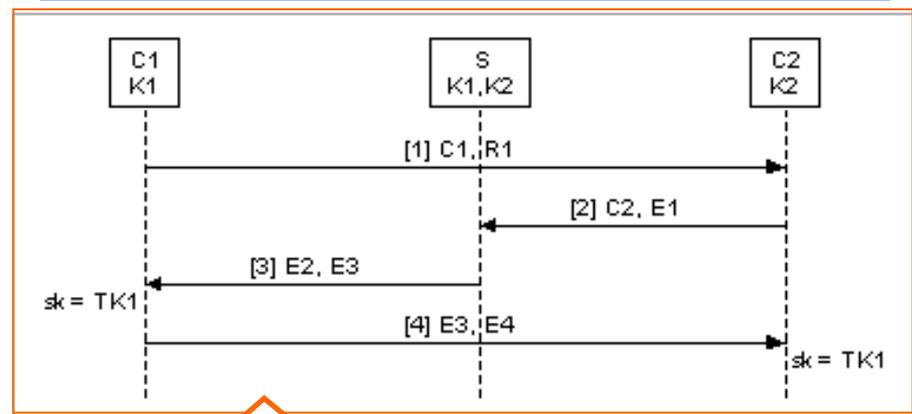
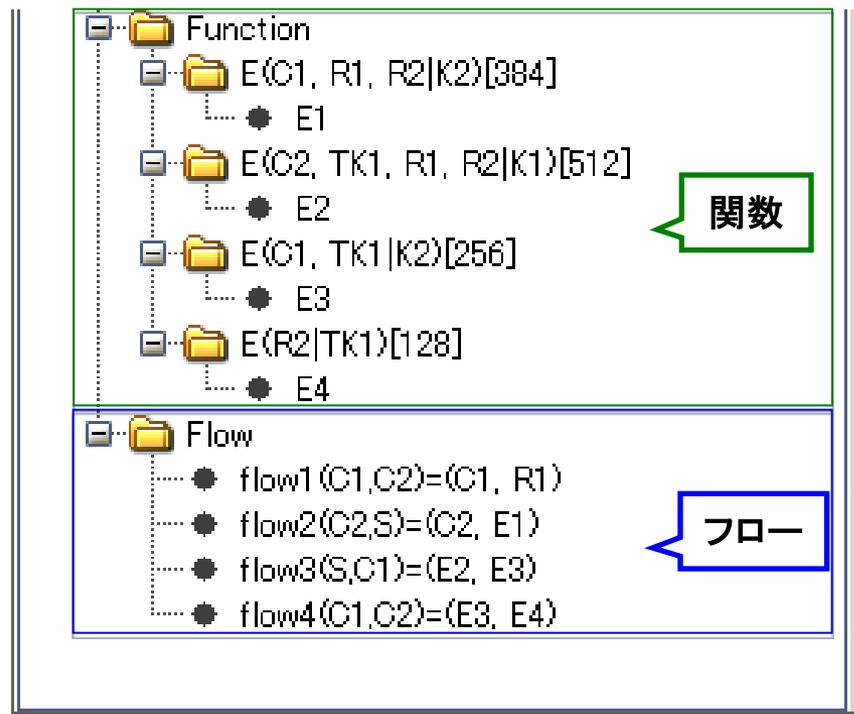
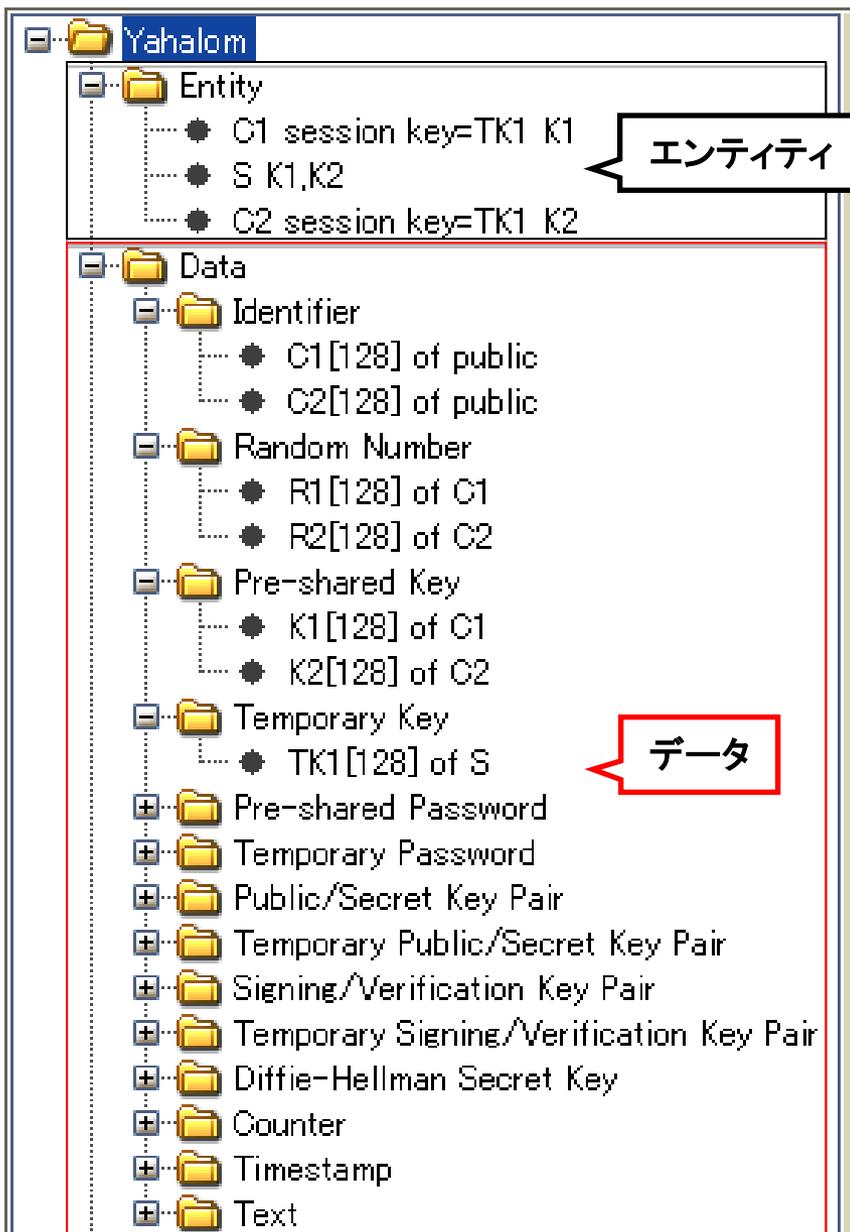
##### メッセージ

評価処理時間: 12.61ミリ秒、  
 観交換プロトコルとして評価: NG  
 観交換プロトコルとして評価: NG  
 危険化チェック: OK  
 長さチェック: OK  
 なりすまし攻撃安全(MC-SIA): OK  
 観交換なりすまし攻撃安全(MC-RKCI with C1): NG  
 観交換なりすまし攻撃安全(MC-RKCI with C2): NG  
 観交換的攻撃安全(SS-SFA): OK  
 観交換的攻撃安全(SS-SAA): OK  
 既知観交換安全(SS-RKS): OK  
 未知観交換安全(SS-RUKS): OK  
 Weak Forward Secrecy(SS-WFS): NG  
 Strong Forward Secrecy(SS-SFS): NG  
 オフライン観交換安全(RODA): N/A  
 観出不可可能なオンライン観交換安全(ROODA): N/A  
 観号プリミティブ(M1-MAC, M2-MAC, M3-MAC)  
 危険化している観交換-[]  
 観交換子(FAQ)-(C1-M2, C2-M1)  
 観交換成順値(FKZ)-(C1-M3, C2-M3)  
 セッション観交換-(C1-M3, C2-M3)  
 セッション観交換成順値タイムスタンプ-(C1-フロー[2]直後, C2-フロー[1]直後)  
 一時データ削除タイムスタンプ(C1)-(R1-フロー[1]直後, R2-フロー[2]直後, R3-フロー[3]直後)  
 一時データ削除タイムスタンプ(C2)-(R1-フロー[2]直後, R2-フロー[2]直後, R3-フロー[2]直後)  
 パスワードを含む観交換-[]  
 引数(SS-SFA)-(M3-[])  
 引数(SS-SAA)-(M3-[M1])  
 引数(RODA)-[]  
 引数(FAQ)-[M1-[], M2-[]]  
 その他(SS-SFA)-[]  
 その他(SS-SAA)-[]  
 その他(RODA)-[]  
 その他(FAQ)-[]  
 [MC-SIA] OK (g,f)-[M2-[[g:null, f:M2]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [MC-RKCI with C1] NG (g,f)-[M2-[[g:null, f:M2]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [MC-RKCI with C2] NG (g,f)-[M2-[[g:null, f:M2]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [SS-SFA] OK (g,f)-[M3-[[g:null, f:M3]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [SS-SAA] OK (g,f)-[M3-[[g:null, f:M3], [g:M3, f:M1]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [SS-RKS] OK (g,f)-[M3-[[g:null, f:M3], [g:M3, f:M1]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [SS-RUKS] OK (g,f)-[M3-[[g:null, f:M3], [g:M3, f:M1]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [SS-WFS] NG (g,f)-[M3-[[g:null, f:M3], [g:M3, f:M1]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)  
 [SS-SFS] NG (g,f)-[M3-[[g:null, f:M3], [g:M3, f:M1]]]  
 type-status-(K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS)

## 検証結果(GUI ベース)

# プロトコルの例 (Yahalom)





シーケンス図

## 評価結果

### メッセージ

評価処理時間: 15.314ミリ秒。

認証プロトコルとして評価: NG

鍵交換プロトコルとして評価: NG

危険化チェック: OK

長さチェック: OK

なりすまし攻撃安全 (MC-SIA): OK

鍵漏洩なりすまし攻撃安全 (MC-RKCI for C1 with S): NG

鍵漏洩なりすまし攻撃安全 (MC-RKCI for C1 with C2): NG

鍵漏洩なりすまし攻撃安全 (MC-RKCI for S with C1): N/A

鍵漏洩なりすまし攻撃安全 (MC-RKCI for S with C2): N/A

鍵漏洩なりすまし攻撃安全 (MC-RKCI for C2 with C1): OK

鍵漏洩なりすまし攻撃安全 (MC-RKCI for C2 with S): NG

受動的攻撃安全 (SS-SPA): OK

能動的攻撃安全 (SS-SAA): OK

既知鍵攻撃安全 (SS-KKS): OK

未知鍵共有攻撃安全 (SS-RUKS): OK

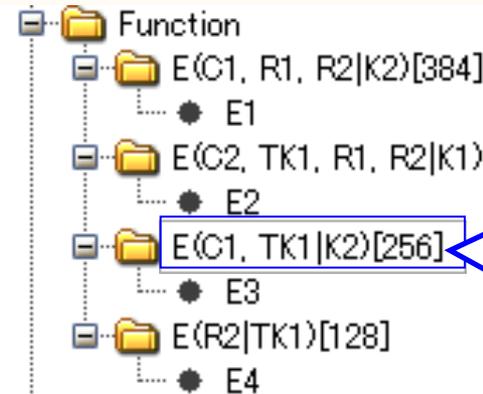
Weak Forward Secrecy (SS-WFS): NG

Strong Forward Secrecy (SS-SFS): NG

鍵プライバシー (SS-KP): N/A

安全でないと判定。

攻撃者は鍵 K2 を知っているため、セッション鍵 TK1 も得られる。



セッション鍵 TK1 は鍵 K2 により暗号化されている。

```
[SS-WFS] NG (E4), [g:E4, f:E2], [g:E4, f:E3]]}
type-status={E1=TV-PS, E2=TV-PS, E3=TV-PS, E4=TV-PS, C1=ID-PS, C2=ID-PS,
K1=LLK-PS, K2=LLK-PS, TK1=TK-PS, R1=ID-PS, R2=ID-PS}
```

# 少し複雑なプロトコル(IKE-PKE)

$SK_P, PK_P, PK_S, X_P, g^{X_P}$

$SK_S, PK_S, PK_P, X_S, g^{X_S}$

**P**

**S**

•CKY-Pを生成し、HDRにセット  
•SAを複数提案

•SK<sub>Y</sub>: ロール Y の秘密鍵  
•PK<sub>Y</sub>: ロール Y の公開鍵  
•X<sub>Y</sub>: ロール Y の Diffie-Hellman 秘密鍵

HDR, SA

HDR, SA

•CKY-Sを生成し、HDRにセット  
•SAを1つ選択

•  $g^{X_P}$ をKEにセット  
•  $ID_P$ をSの公開鍵で暗号化  
• ナンス  $N_P$ を生成し、Sの公開鍵で暗号化

{Z}PK<sub>Y</sub>: 公開鍵 PK<sub>Y</sub> による Z の暗号化

HDR, KE, [HASH(1)],  
{ID<sub>P</sub>}PK<sub>S</sub>, {N<sub>P</sub>}PK<sub>S</sub>

•  $g^{X_S}$ をKEにセット  
•  $ID_S$ をPの公開鍵で暗号化  
• ナンス  $N_S$ を生成し、Pの公開鍵で暗号化

HDR, KE,  
{ID<sub>S</sub>}PK<sub>P</sub>, {N<sub>S</sub>}PK<sub>P</sub>

•  $g^{X_P X_S}$ を共有 ←  $(g^{X_S})^{X_P}$   
• SKEYIDを導出 ←  $prf(hash(N_P || N_S), CKY-P || CKY-S)$

•  $g^{X_P X_S}$ を共有 ←  $(g^{X_P})^{X_S}$   
• SKEYIDを導出 ←  $prf(hash(N_P || N_S), CKY-P || CKY-S)$

• HASH<sub>P</sub>を計算 ←  $prf(SKEYID, g^{X_P} || g^{X_S} || CKY-P || CKY-S || SA_P || ID_P)$

HDR\*, HASH<sub>P</sub>

• HASH<sub>S</sub>を計算 ←  $prf(SKEYID, g^{X_S} || g^{X_P} || CKY-S || CKY-P || SA_P || ID_S)$

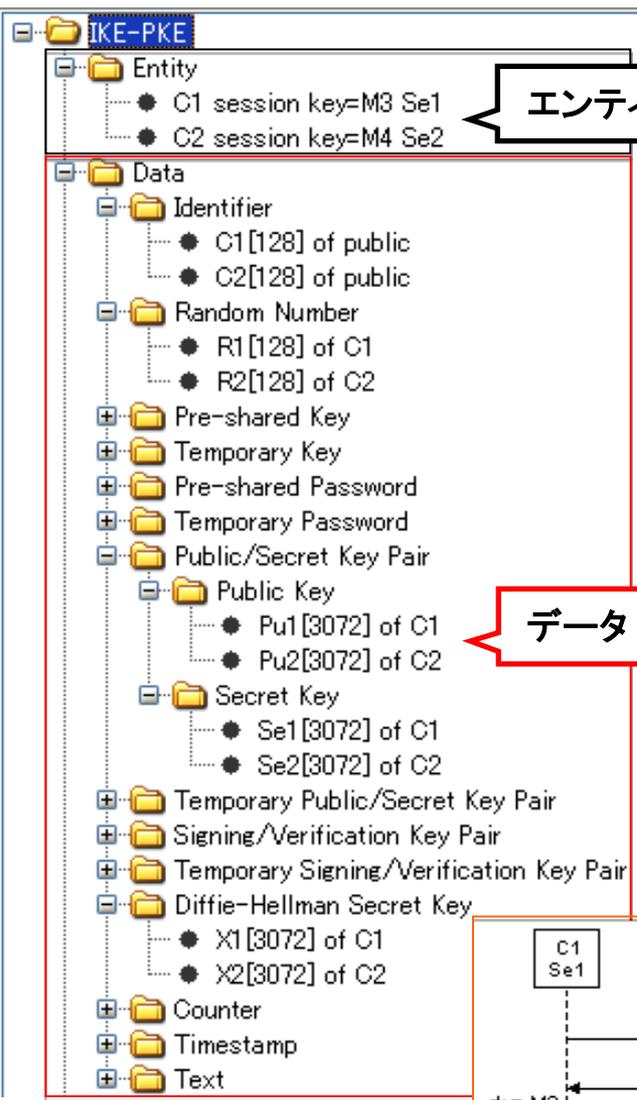
HDR\*, HASH<sub>S</sub>

sk=SKEYID<sub>e</sub>

sk=SKEYID<sub>e</sub>

• SKEYID<sub>d</sub> ←  $prf(SKEYID, g^{X_P X_S} || CKY-P || CKY-S || 0)$   
• SKEYID<sub>a</sub> ←  $prf(SKEYID, SKEYID_d || g^{X_P X_S} || CKY-P || CKY-S || 1)$   
• SKEYID<sub>e</sub> ←  $prf(SKEYID, SKEYID_a || g^{X_P X_S} || CKY-P || CKY-S || 2)$   
• [ ]: SKEYID<sub>e</sub>によって暗号化されたペイロード

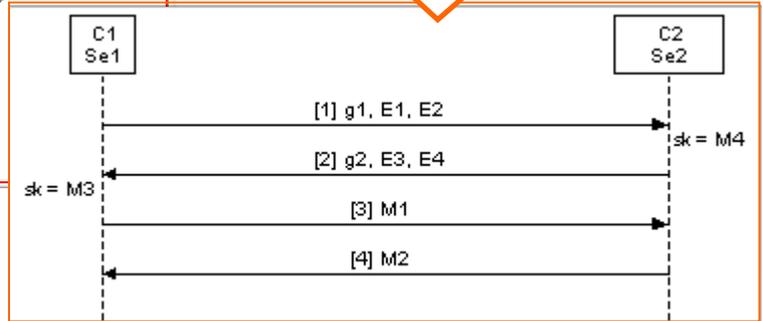
セッション鍵 SKEYID<sub>e</sub>



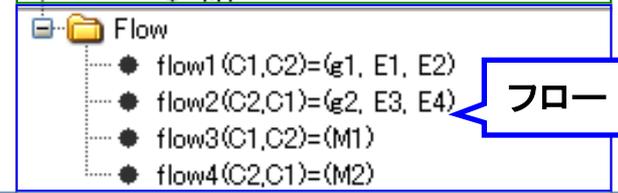
エンティティ

データ

シーケンス図



関数



フロー

## 評価結果

### メッセージ

評価処理時間: 22.467ミリ秒。

認証プロトコルとして評価: OK

鍵交換プロトコルとして評価: OK

危殆化チェック: OK

長さチェック: OK

なりすまし攻撃安全 (MC-SIA): OK

鍵漏洩なりすまし攻撃安全 (MC-RKCI with C1): OK

鍵漏洩なりすまし攻撃安全 (MC-RKCI with C2): OK

受動的攻撃安全 (SS-SPA): OK

能動的攻撃安全 (SS-SAA): OK

既知鍵攻撃安全 (SS-KKS): OK

未知鍵共有攻撃安全 (SS-RUKS): OK

Weak Forward Secrecy (SS-WFS): OK

Strong Forward Secrecy (SS-SFS): OK

KDDI 研独自ツールにおいて検証可能なすべての安全性を満足すると判定。

## ➤ プロトコル仕様

- 仕様の不明確さなどのために、**どのように入力されるか**に依存して、検証結果が変わる可能性あり。

## ➤ モデル記述

- **どの情報を入力すると正しく検証されるのか**のノウハウが必要。
- プロトコル情報の**モデル化により**、検証結果が変わる可能性あり。
- **モデル化の正当性・妥当性**を別途評価する必要あり。

## ➤ 評価の実行および結果の解釈

- **認証子やセッション鍵**を設定する必要があり、認証子やセッション鍵が明確でない場合には検証結果が変わる可能性あり。
- 一部の特殊なプロトコルでは、**鍵生成関数や引数**などを別途設定しなければならないが、そのノウハウが必要。
- 検証結果の**詳細ログを読み解く**にはノウハウが必要であり、安全でないと判定された場合の**脆弱性の理解**にもノウハウが必要。
- **検証結果の正当性・妥当性**を別途評価する必要あり。

## ➤ ツールの制約

- データや関数種別が決まっているので、種別でない情報を入力不可。
- 「その他の関数」を選択可能であるが、検証結果が正しくない可能性あり。
- 規定されたセキュリティプロパティ以外の安全性を検証不可で、規定されたセキュリティプロパティ内でも、さらに分類した安全性を検証不可。
- 2種類以上の認証子やセッション鍵を設定不可。
- 長さが明確に定義されている関数の出力値の一部だけを使用するような設定不可。

## ➤ その他

- パスワードベースを除く認証プロトコルでは、2種類の安全性しかなく、攻撃者モデルを詳細化する必要あり。